Secret key········ In prior to correspondence, ········ Secret key
Symmetric secret key possessed

Plain text → Encryption → Network / Cypher text → Decryption → Original Plain text

Sender A

Receiver B

(a) Common key encryption

(All senders)

B's public key ········ Published in B`s homepages etc. ········ B's secret key

Plain text → Encryption → Network / Cypher text → Decryption → Plain text

Sender X

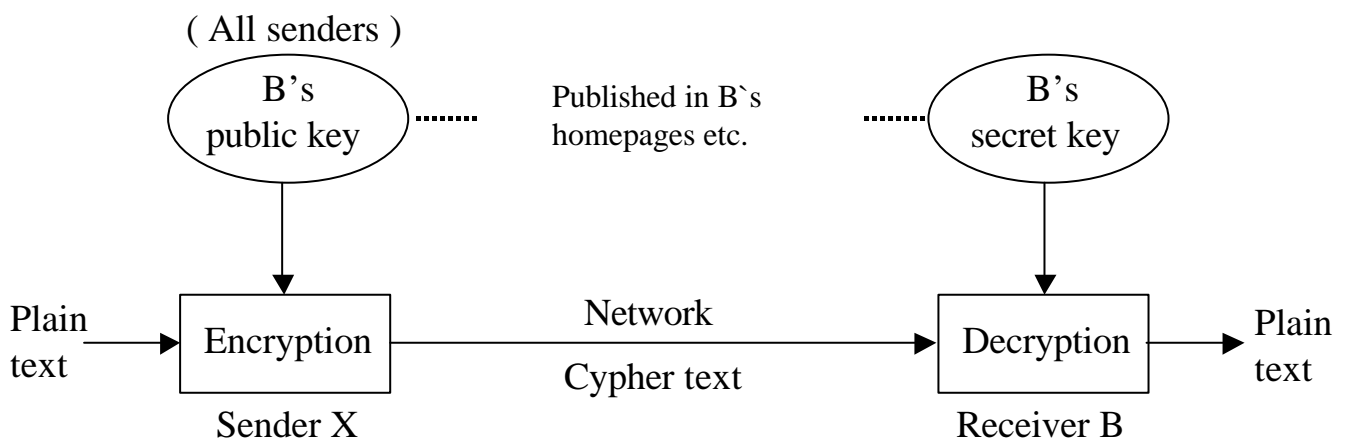Receiver B

(b) Public key encryption

Fig 1   Symmetric key cryptosystem + Public-key cryptosystem

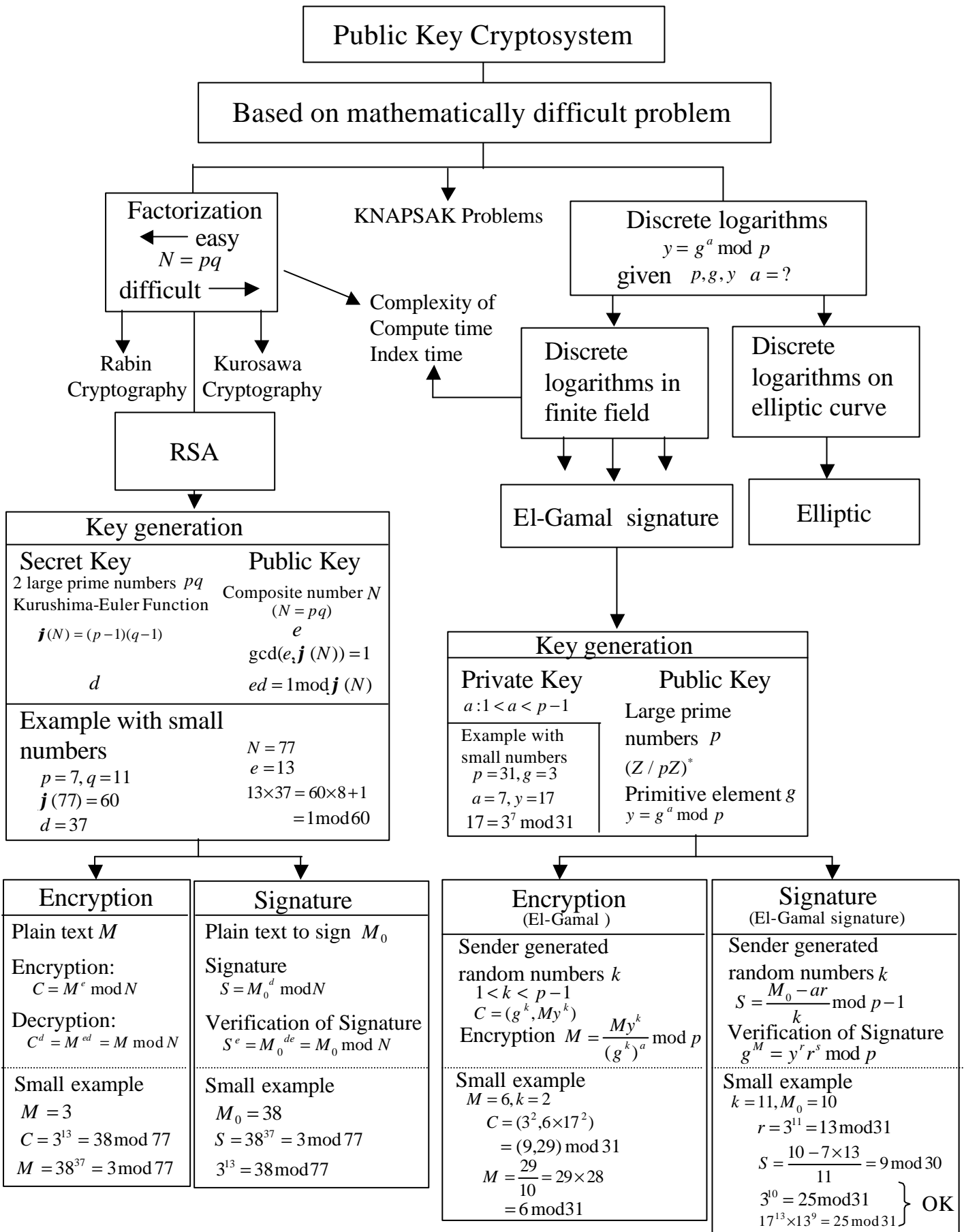# Public Key Cryptosystem

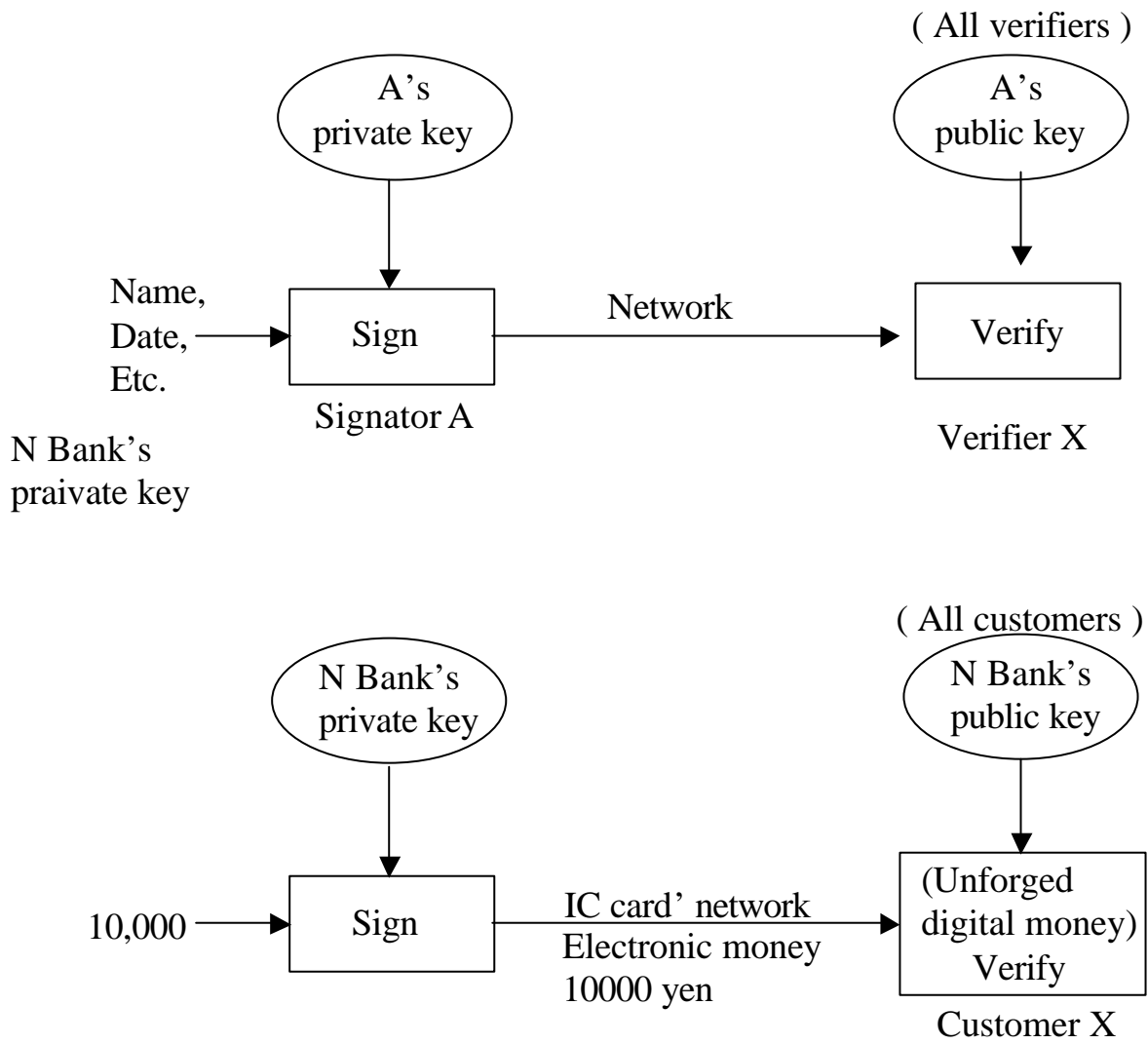## Based on mathematically difficult problem

Factorization
$\leftarrow$ easy
$N = pq$
difficult $\rightarrow$

KNAPSAK Problems

Discrete logarithms
$y = g^a \bmod p$
given $p, g, y \quad a = ?$

Complexity of
Compute time
Index time

Rabin Cryptography

Kurosawa Cryptography

RSA

Discrete logarithms in finite field

Discrete logarithms on elliptic curve

El-Gamal signature

Elliptic

Key generation

Secret Key	Public Key
2 large prime numbers pq	Composite number N
Kurushima-Euler Function	$(N = pq)$
$\boldsymbol{j}(N) = (p-1)(q-1)$	e
	$\gcd(e, \boldsymbol{j}(N)) = 1$
d	$ed = 1 \bmod \boldsymbol{j}(N)$

Example with small numbers

$p = 7, q = 11$ $N = 77$
$\boldsymbol{j}(77) = 60$ $e = 13$
$d = 37$ $13 \times 37 = 60 \times 8 + 1$
   $= 1 \bmod 60$

Key generation

Private Key	Public Key
$a : 1 < a < p-1$	Large prime numbers p
Example with small numbers	$(Z/pZ)^*$
$p = 31, g = 3$	Primitive element g
$a = 7, y = 17$	$y = g^a \bmod p$
$17 = 3^7 \bmod 31$	

Encryption

Plain text M

Encryption:
$C = M^e \bmod N$

Decryption:
$C^d = M^{ed} = M \bmod N$

Small example
$M = 3$
$C = 3^{13} = 38 \bmod 77$
$M = 38^{37} = 3 \bmod 77$

Signature

Plain text to sign M_0

Signature
$S = M_0^{\,d} \bmod N$

Verification of Signature
$S^e = M_0^{\,de} = M_0 \bmod N$

Small example
$M_0 = 38$
$S = 38^{37} = 3 \bmod 77$
$3^{13} = 38 \bmod 77$

Encryption (El-Gamal)

Sender generated random numbers k
$1 < k < p-1$
$C = (g^k, My^k)$
Encryption $M = \dfrac{My^k}{(g^k)^a} \bmod p$

Small example
$M = 6, k = 2$
$C = (3^2, 6 \times 17^2)$
$= (9, 29) \bmod 31$
$M = \dfrac{29}{10} = 29 \times 28$
$= 6 \bmod 31$

Signature (El-Gamal signature)

Sender generated random numbers k
$S = \dfrac{M_0 - ar}{k} \bmod p-1$
Verification of Signature
$g^M = y^r r^s \bmod p$

Small example
$k = 11, M_0 = 10$
$r = 3^{11} = 13 \bmod 31$
$S = \dfrac{10 - 7 \times 13}{11} = 9 \bmod 30$
$3^{10} = 25 \bmod 31$
$17^{13} \times 13^9 = 25 \bmod 31$ $\Big\}$ OK

Fig.2   Public Key Cryptosystem

A's
private key

(All verifiers)
A's
public key

Name,
Date,
Etc. → Sign → Network → Verify

Signator A

Verifier X

N Bank's
praivate key

N Bank's
private key

(All customers)
N Bank's
public key

10,000 → Sign → IC card' network
Electronic money
10000 yen → (Unforged
digital money)
Verify

Customer X

Fig 3   Authentication digital signature by public key cryptography

Long plaintext
————
————
————
Date,Time,Name

Compression

Plaintext

Plaintext

Hash

Hashed value

Signed text

Signature

Network

Plaintext,
Signed text

A's secret key

Signator A

Long plaintext
————
————
————
Date,Time,Name

Plaintext

Plaintext

Hash

Hashed value

Decryption

Hashed value

= ?
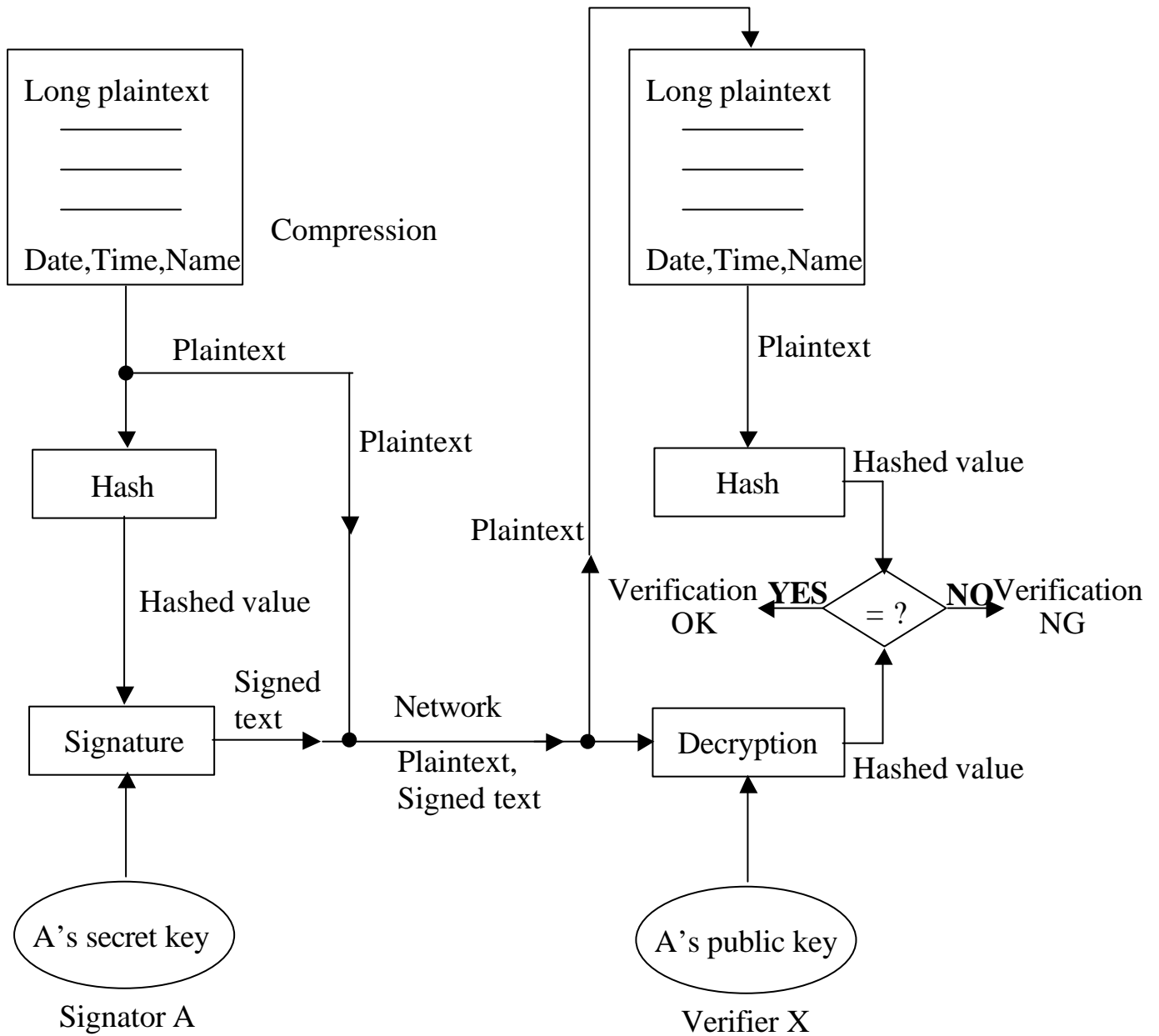
YES Verification OK

NO Verification NG

A's public key

Verifier X

Fig 4: Digital signature system [1]